

REMARKS

Claims 1-10 and 13-29 were presented for examination and were pending in this application. In an Official Action dated May 4, 2005, claims 1-10 and 13-29 were rejected. Applicants herein cancel claims 1-10 and 13-29. Applicants herein add new claims 30-55. Applicants thank Examiner for examination of the claims pending in this application and addresses Examiner's comments below.

Response to Rejection Under 35 USC 102(e)

In the 4th paragraph of the Office Action, Examiner rejected claims 1-10 and 13-29 under 35 USC § 102(e) as allegedly being anticipated by U.S. Patent No. 6,473,800 to Jerger et al. ("Jerger"). This rejection is now traversed. Generally, while claim 30 recites vulnerability detection rules for targeted intrusion detection monitoring with intrusion detection rules, Jerger only discloses security zones for downloading active content.

More specifically, Jerger discloses a method for managing active content downloaded from a computer network. (See Abstract). The portion of Jerger relied on by Examiner further discloses that security zones are configured, each zone specifying actions to be taken when a protected operation is requested by the active content. (See col. 3, ll. 5-24). Jerger goes on to disclose certain procedures that are followed prior to performing the protected operation.

Claim 30 recites a method for use on a network to analyze a network resource from a remote location. The steps of the method comprise:

- providing vulnerability detection rules for determining at least one of an application and an operating system on the network resource, and for selecting vulnerabilities associated with the at least one of the determined application and the determined operating system, based on responses from the network resource satisfying conditions of the vulnerability detection rules; and
- providing intrusion detection rules, corresponding to the selected vulnerabilities, for examining network traffic for attacks on the at least one of the application and the operating system responsive to the network traffic satisfying conditions of the intrusion detection rules.

Advantageously, the rules can provide targeted monitoring for an intrusion detection system, i.e., monitoring for determined vulnerabilities associated with operating systems and applications known to be present on a network resource, rather than unwittingly monitoring for all potential vulnerabilities associated with a network. Furthermore, the rules provide a simplified construction of rules for these purposes.

However, Jerger fails to teach or suggest the method of claim independent 30. Specifically, whereas claim 30 provides vulnerability detection rules that can detect a specific application or a specific operating system, the security zones of Jerger only detect active content downloads without regard to the application or the operating system on a network resource. Additionally, the vulnerability detection rules of claim 30 can select specific vulnerabilities that are likely to exist on the network resource, but Jerger can only be manually configured for reaction to a single action—active content downloads. Furthermore, although claim 30 provides intrusion detection rules that correspond to selected vulnerabilities, Jerger merely determines whether to allow access to a general class of protected operations accessed by the active content. Therefore, Jerger fails to teach or suggest the features recited in independent claim 30. Applicants respectfully submit that claim 30 is in condition for allowance.

To the extent that other independent claims, and related dependent claims, contain similar features, these claims are allowable for at least the same reasons.

CONCLUSION

In sum, Applicants respectfully submit that claims 30-55, as presented herein, are patentably distinguishable over the cited references. Therefore, Applicants request reconsideration of the basis for the rejections to these claims and request allowance of them.

In addition, Applicants respectfully invite Examiner to contact Applicants' representative at the number provided below if Examiner believes it will help expedite furtherance of this application.

Respectfully Submitted,
JOHN S. FLOWERS, ET AL.

Date:

10/4/05

By:



Dorian Cartwright, Attorney of Record
Registration No. 53,853
FENWICK & WEST LLP
801 California Street
Mountain View, CA 94041
Phone: (650) 335-7247
Fax: (650) 938-5200
E-Mail: dcartwright@fenwick.com